PATENT APPLICATION
DOCKET NO. 200311942-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTOR(S): Curtis Reese **GROUP ART UNIT:** 2609

SERIAL NO.: 10/700,205 **EXAMINER:** Wills, Lawrence E.

FILED: 11/03/2003

SUBJECT: PRINTER ACCESS CONTROL

COMMISSIONER FOR PATENTS
ALEXANDRIA, VA 22313-1450

SIR:

APPELLANTS'/APPLICANTS' OPENING BRIEF ON APPEAL

1. REAL PARTY IN INTEREST.

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holding, LLC.

2. RELATED APPEALS AND INTERFERENCES.

There are no other appeals or interferences known to Appellants, Appellants' legal representative or the Assignee which will affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS.

Claims 1-9, 13-21, and 25-33 are pending but stand rejected. Claims 10-12, 22-24, and 34-36 have been cancelled. The rejections of all pending claims are appealed.

4. STATUS OF AMENDMENTS.

No amendments have been filed after the final action was entered. All previous amendments have been entered.

5. SUMMARY OF CLAIMED SUBJECT MATTER.

Claim 1 recites a printer access control module within a printer that is operable to implement a method. That method includes receiving a request from a client computer for printing resource authorization. *See, e.g.,* Specification, page 5, lines 1-7 and Fig. 2, step 202. The policy domain of the requesting client computer is determined. *See, e.g.,* Specification, page 5, lines 1-7 and Fig. 2, step 203. A security key is issued to the client device, the security key indicative of one or more printer resources available to client computers of the determined

policy domain. *See, e.g.*, Specification, page 4, lines 25-34, page 5, lines 8-12, page 6, lines 15-23, and Fig. 2, step 204. A print job received from the client computer is authorized to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job. *See, e.g.*, Specification, page 6, lines 9-23 and Fig. 2, steps 207-209.

Claim 13 recites a printer that is operable to implement a method. That method includes receiving a request from a client computer for printing resource authorization. *See, e.g.*, Specification, page 5, lines 1-7 and Fig. 2, step 202. A policy domain of the requesting client computer is determined. *See, e.g.*, Specification, page 5, lines 1-7 and Fig. 2, step 203. A security key is issued to the client device. The security key is indicative of one or more printer resources available to client computers of the determined policy domain. *See, e.g.*, Specification, page 4, lines 25-34, page 5, lines 8-12, page 6, lines 15-23, and Fig. 2, step 204. A print job received from the client computer is authorized to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job. *See, e.g.*, Specification, page 6, lines 9-23 and Fig. 2, steps 207-209.

Claim 25 recites a machine-readable medium with instructions stored thereon, the instructions when executed on a computerized system operable to cause the system to implement a method. That method includes receiving a request from a client computer for printing resource authorization. *See, e.g.*, Specification, page 5, lines 1-7 and Fig. 2, step 202. The policy domain of the requesting client computer is determined. *See, e.g.*, Specification, page 5, lines 1-7 and Fig. 2, step 203. A security key is issued to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain. *See, e.g.*, Specification, page 4, lines 25-34, page 5, lines 8-12, page 6, lines 15-23, and Fig. 2, step 204. A print job received from the client computer is authorized to be printed using one or more printer resources indicated by the issued security key used by the client computer to

encrypt the print job. *See, e.g.*, Specification, page 6, lines 9-23 and Fig. 2, steps 207-209.

6. GROUNDS FOR REJECTION TO BE REVIEWED.

A. Claims 1-7, 13-19, and 25-31 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USPN 6,490,049 issued to Cunnagin.

B. Claims 8, 9, 20, 21, 32, and 33 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USPN 6,490,049 issued to Cunnagin and in further view of USPN 6,545,767.

7. ARGUMENT.

A. Ground For Rejection A – Claims 1-7, 13-19, and 25-31 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USPN 6,490,049 issued to Cunnagin.

Claim 1 is directed to a printer access control module within a printer that is operable to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

Tanimoto, as admitted by the Examiner, does not teach the use of security keys key that are (a) indicative of one or more printer resources available to client computers of the determined policy domain and (b) used to encrypt a print job. At page 3 of the final office action, the Examiner attempts to overcome Tanimoto's deficiency stating:

> Cunnagin '049 teaches issue a security key to the client device (i.e. as shown in Fig. 1, the access control key is requested by the printer in Step 52. Thus, the security key must be issued to the client. In view of this, "issue a security key to the client device" is an inherent feature of Cunnagin' 049) and the issued security key used by the client computer to encrypt the print job (i.e. stored as an encrypted data file in column 4, line 13).

Claim 1 plainly recites that the print job being authorized is a print job that has been encrypted with a security key and that security key is indicative of one or more printer resources available to a client device. Cunnagin, col. 4, lines 1-22 and Fig. 2, on the other hand, describes a system in which a user of a host computer can change the mode of operation of a printer. Using a printer driver, the user accesses a display screen and selects a desired mode. To initiate the request, the user must enter a password. The password entered by the user is compared against a "correct password." The "correct password' is either stored in an encrypted file on the host computer or on the printer itself. Once a user enterers a password via the display screen and that password is determined to match the "correct password" stored in the encrypted file or on the printer, the user is allowed to change the printer's mode of operation.

The examiner mistakenly equates Cunnagin's encrypted file that stores the "correct password" with the print job encrypted with a security key recited in Claim 1. Cunnagin encrypted file is not a print job. It is simply a file containing a password that is encrypted to obscure the password from view of a user of the host computer. In fact Cunnagin mentions nothing of print jobs. Consequently, Cunnagin, like Tanimoto, fails to teach or suggest the use of security key,

indicative of one or more printer resources available to client computers, that is used to encrypt a print job.

Therefore, Tanimoto even when combined with Cunnagin fails to teach or suggest a printer access control module within a printer that is operable to authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job. For at least these reasons Claim 1 and Claims 2-9 which depend from Claim 1 are patentable over the cited art.

Claim 13 is directed to a printer that is operable to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

As with Claim 1, neither Cunnagin nor Tanimoto , individually or combined, teaches or suggests a printer that is operable to authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job. For at least the same reasons Claim 1 is patentable, so are Claim 13 and Claims 14-21which depend from Claim 13.

Claim 25 is directed to a machine-readable medium with instructions stored thereon, the instructions when executed on a computerized system operable to cause the system to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

As with Claim 1, neither Cunnagin nor Tanimoto , individually or combined, teaches or suggests authorizing a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job. For at least the same reasons Claim 1 is patentable, so are Claim 25 and Claims 26-33 which depend from Claim 25.

B. Ground For Rejection B – Claims 8, 9, 20, 21, 32, and 33 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USPN 6,490,049 issued to Cunnagin and in further view of USPN 6,545,767.

Claims 8 and 9 depend from Claim 1. Claims 20 and 21 depend from Claim 13. Claims 32 and 33 depend from Claim 25. For at least the same reasons Claims 1, 13, and 25 are patentable so are Claims 5, 8, 9, 20, 21, 32, and 33.

Conclusion

In view of the foregoing remarks and amendments, Applicant respectfully submits that Claims 1-9, 13-21, and 25-33 define allowable subject matter. The Applicant respectfully requests that the Board reverse the rejections, indicate the allowability of all claims in the application and to pass the application to issue.

Respectfully submitted,
Curtis Reese

By /Jack H. McKinney/
Jack H. McKinney
Reg. No. 45,685

January 14, 2008

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. (previously presented) A printer access control module within a printer that is operable to:

receive a request from a client computer for printing resource authorization;

determine the policy domain of the requesting client computer;

issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and

authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job.

2. (previously presented) The printer access control module of claim 1, wherein issuing a security key comprises issuing a security key that is indicative of full printing resource authorization to client computers that are members of a predetermined policy domain and issuing a security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain.

3. (previously presented) The printer access control module of claim 1, wherein issuing a security key comprises issuing a security that is indicative of greater printing resource authorization to client computers that are members of a predetermined policy domain than to client computers that are not members of the predetermined policy domain.

4. (previously presented) The printer access control module of claim 1, wherein one printer resource includes color printing.

5. (previously presented) The printer access control module of claim 1, wherein one printer resource includes printing print jobs over a specified page limit.

6. (previously presented) The printer access control module of claim 1, wherein one or more printer resources include specific print media, specific print media comprising at least one of letterhead, check stock, glossy paper, and transparencies.

7. (previously presented) The printer access control module of claim 1, wherein one or more printer resources include at least one of a maximum cost per page, maximum cost per period of time, and maximum pages per period of time.

8. (original) The printer access control module of claim 1, wherein the policy domain comprises a predefined portion of network node addresses on a local area network

9. (original) The printer access control module of claim 1, wherein the policy domain comprises a predefined group of identifiable users.

10. (cancelled)

11. (cancelled)

12. (cancelled)

13. (previously presented) A printer that is operable to:

receive a request from a client computer for printing resource authorization;

determine the policy domain of the requesting client computer;

issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and

authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job.

14. (previously presented) The printer of claim 13, wherein issuing a security key comprises issuing a security key that is indicative of full printing resource authorization to client computers that are members of a predetermined policy domain and issuing a security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain.

15. (previously presented) The printer of claim 13, wherein issuing a security key comprises issuing a security that is indicative of greater printing resource authorization to client computers that are members of a predetermined policy domain than to client computers that are not members of the predetermined policy domain.

16. (previously presented) The printer of claim 13, wherein one printing resource comprises color printing.

17. (previously presented) The printer of claim 13, wherein one printing resource comprises printing print jobs over a specified page limit.

18. (previously presented) The printer of claim 13, wherein one or more printing resources comprise specific print media, specific print media comprising at least one of letterhead, check stock, glossy paper, and transparencies.

19. (previously presented) The printer of claim 13, wherein one or more printing resources comprise at least one of a maximum cost per page, maximum cost per period of time, and maximum pages per period of time.

20. (original) The printer of claim 13, wherein the policy domain comprises a predefined portion of network node addresses on a local area network

21. (original) The printer of claim 13, wherein the policy domain comprises a predefined group of identifiable users.

22. (cancelled)

23. (cancelled)

24. (cancelled)

25. (previously presented) A machine-readable medium with instructions stored thereon, the instructions when executed on a computerized system operable to cause the system to:

receive a request from a client computer for printing resource authorization;

determine the policy domain of the requesting client computer;

issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain; and

authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job.

26. (previously presented) The machine-readable medium of claim 25, wherein issuing a security key comprises issuing a security key that is indicative

of full printing resource authorization to client computers that are members of a predetermined policy domain and issuing a security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain.

27. (previously presented) The machine-readable medium of claim 25, wherein issuing a security key comprises issuing a security that is indicative of greater printing resource authorization to client computers that are members of a predetermined policy domain than to client computers that are not members of the predetermined policy domain.

28. (previously presented) The machine-readable medium of claim 25, wherein one printing resource comprises color printing.

29. (previously presented) The machine-readable medium of claim 25, wherein one printing resource comprises printing print jobs over a specified page limit.

30. (previously presented) The machine-readable medium of claim 25, wherein one or more printing resource comprises specific print media, specific print media comprising at least one of letterhead, check stock, glossy paper, and transparencies.

31. (previously presented) The machine-readable medium of claim 25, wherein one or more printing resource comprises at least one of a maximum cost per page, maximum cost per period of time, and maximum pages per period of time.

32. (original) The machine-readable medium of claim 25, wherein the policy domain comprises a predefined portion of network node addresses on a local area network.

33. (original) The machine-readable medium of claim 25, wherein the policy domain comprises a predefined group of identifiable users.

34. (original)

35. (original)

36. (original)

Evidence Appendix

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.